Amendments to the Specification:

Please replace the paragraph starting on page 1, line 22, with the following amended paragraph:

In order to recover the data, an authentication certificate normally accompanies the digital signature. The authentication certificate provides a public key corresponding to the private key for use in data recovery and for certifying (or attesting) to something. The meaning of a certificate depends on the contents of the certificate and the empowerment of the certificate signer (issuer). ~~For example, the attestation may indicate that a given signature private key was installed in protected hardware, especially an isolated execution architecture designed below.~~

Please replace the paragraph starting on page 3, line 2, with the following amended paragraph:

The features and advantages of the present invention will become apparent from the following detailed description of one or more example embodiments of the present invention in which:

Please replace the paragraph starting on page 4, line 2, with the following amended paragraph:

The present invention relates to a platform and method for certifying a key within protected hardware. Herein, certain details are set forth in order to provide a thorough understanding of the present invention. It is apparent to a person of ordinary skill in the art, however, that the present invention may be practiced through many embodiments other ~~that~~ than those illustrated. Well-known circuits and hashing techniques are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

Please replace the paragraph starting on page 5, line 6, with the following amended paragraph:

One principle for enhancing security ~~of transmitted~~ is through configuration of the platform with an isolated execution (ISOX™) architecture. The ISOX™ architecture includes logical and physical definitions of hardware and software components that interact directly or indirectly with an operating system of a platform. Herein, the operating system and a processor of the platform may have several levels of hierarchy, referred to as rings, which correspond to various operational modes. A "ring" is a logical division of hardware and software components that are designed to perform dedicated tasks within the operating system. The division is typically based on the degree or level of privilege, namely the ability to make changes to the platform. For example, a ring-0 is the innermost ring, being at the highest level of the hierarchy. Ring-0 encompasses the most critical, privileged components. Ring-3 is the outermost ring, being at the lowest level of the hierarchy. Ring-3 typically encompasses user level applications, which are normally given the lowest level of privilege. Ring-1 and ring-2 represent the intermediate rings with decreasing levels of privilege.

Please replace the paragraph starting on page 11, line 6, with the following amended paragraph:

The processor nub loader 52, as shown in Figures 1A and 1C, includes a processor nub loader code and its hash value (or digest). After being invoked by execution of an ~~appropriated~~ appropriate isolated instruction (e.g., ISO-INIT) by the processor 110, the processor nub loader 52 is transferred to the isolated area 70. Thereafter, the processor nub loader 52 copies the processor nub 18 from the non-volatile memory 160 into the isolated area 70, verifies and places the hash value of the processor nub 18 into an audit log of the hardware-protected memory 152 as described below. In one embodiment, the hardware-protected memory 152 is implemented as any memory array with single write, multiple read capability. This non-modifiable capability is controlled by logic or is part of the inherent nature of the memory itself. For example, as shown, the protected memory 152 may include a plurality of single write, multiple read registers.

Please replace the paragraph starting on page 12, line 11, with the following amended paragraph:

The cryptographic key storage 154 holds a symmetric key that is unique for the platform 100. In one embodiment, the cryptographic key storage 154 includes internal fuses that are programmed at manufacturing. Alternatively, the symmetric key contained in the cryptographic key storage 154 may ~~create~~ be created with the aid of a random number generator.